**AFRL-RI-RS-TM-2008-16**
**Final Technical Memorandum**
**April 2008**

# ADVANCED COURSE IN ENGINEERING (ACE) - CYBER SECURITY BOOT CAMP

**Syracuse University**

**STINFO COPY**

**AIR FORCE RESEARCH LABORATORY**
**INFORMATION DIRECTORATE**
**ROME RESEARCH SITE**
**ROME, NEW YORK**

# NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the Air Force Research Laboratory Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TM-2008-16 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/

SCOTT ADAMS
Work Unit Manager

/s/

WARREN H. DEBANY, Jr.
Technical Advisor, Information Grid Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

# REPORT DOCUMENTATION PAGE

*Form Approved*
**OMB No. 0704-0188**

| | | |
|---|---|---|
| **1. REPORT DATE** *(DD-MM-YYYY)*<br>APR 08 | **2. REPORT TYPE**<br>Final | **3. DATES COVERED** *(From - To)*<br>Apr 05 – Sep 07 |

**4. TITLE AND SUBTITLE**

ADVANCED COURSE IN ENGINEERING (ACE) – CYBER SECURITY BOOT CAMP

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**
FA8750-05-2-0123

**5c. PROGRAM ELEMENT NUMBER**
63789F

**6. AUTHOR(S)**

Susan Older

**5d. PROJECT NUMBER**
CSAE

**5e. TASK NUMBER**
00

**5f. WORK UNIT NUMBER**
01

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Syracuse University - EECS Dept
Office of Sponsored Programs
113 Bowne Hall
Syracuse NY 13244-1200

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

AFRL/RIGB
525 Brooks Rd
Rome NY 13441-4505

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSORING/MONITORING AGENCY REPORT NUMBER**
AFRL-RI-RS-TM-2008-16

**12. DISTRIBUTION AVAILABILITY STATEMENT**
*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# WPAFB 08-2296*

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The goal of the Advanced Course in Engineering on Cyber Security (ACE) was to develop next-generation cyber-security leaders, with a particular emphasis on educating future military leaders. ACE sought the best students at United States colleges and universities for this endeavor. ACE achieved its stated objectives by completely immersing students in the cyber-security discipline for ten weeks, through a combination of intense coursework, open-ended problems, and internship experiences at local government and industry cyber-security labs. While providing real-world problems, the ACE faculty taught the students to formulate clear problem statements, make reasonable assumptions, apply engineering tools and techniques, solve the problems to a certain depth, apply risk analysis to the solutions, and deliver those solutions on time. In addition to solving problems and delivering solutions on time, students learned to communicate through written reports and compelling presentations.

**15. SUBJECT TERMS**

Cyber Security education, technical leadership development

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON**<br>Scott F. Adams |
|---|---|---|---|---|---|
| **a. REPORT**<br>U | **b. ABSTRACT**<br>U | **c. THIS PAGE**<br>U | UL | 15 | **19b. TELEPHONE NUMBER (*Include area code)***<br>N/A |

# Abstract

The goal of the Advanced Course in Engineering on Cyber Security (ACE) was to develop the next-generation cyber-security leaders, with a particular emphasis on educating future military leaders. ACE sought the best students at United States colleges and universities for this endeavor.

ACE achieved its stated objectives by completely immersing students in the cyber-security discipline for ten weeks, through a combination of intense coursework, open-ended problems, and internship experiences at local government and industry cyber-security labs. While providing real-world problems, the ACE faculty taught the students to formulate clear problem statements, make reasonable assumptions, apply engineering tools and techniques, solve the problems to a certain depth, apply risk analysis to the solutions, and deliver those solutions on time. In addition to solving problems and delivering solutions on time, students learned to communicate through written reports and compelling presentations.

# Contents

# 1 Summary

The Advanced Course in Engineering on Cyber Security (ACE) sought to develop the next-generation cyber security leaders from the best students at United States (US) colleges and universities. It targeted the top students in computer-related disciplines. The course taught them to become original thinkers, problem solvers and technical leaders.

The ACE achieved its stated objectives through focused instruction with strong emphasis on problem solving. Faced with real-world problems, the ACE faculty taught the students to formulate clear problem statements, make reasonable assumptions, apply engineering tools and techniques, solve the problems to a certain depth, apply risk analysis to the solutions, and deliver those solutions on time. In addition to solving problems and delivering solutions on time, students learned to communicate through written reports and compelling presentations.

Taught under the auspices of the Griffiss Institute in Rome, the ACE partnership included Syracuse University, the United States Military Academy (USMA) at West Point, ITT Corporation, and the Information Directorate at the Air Force Research Laboratory (AFRL). The faculty was drawn from academia, government and industry, and provided the students with broad cyber security experiences.

Besides teaching a broad curriculum on cyber security, the ACE placed the students with AFRL where they contributed their newfound knowledge to ongoing research and development projects. A capstone Hackfest also permitted the students as well as AFRL personnel to put into practice many of the lessons learned in the course, to test state-of-the-art tools, and to gather data for use in ongoing activities.

# 2 Introduction

In his introduction of The National Strategy to Secure Cyberspace, President George W. Bush wrote that "securing cyberspace is an extraordinarily difficult strategic challenge that requires coordinated and focused effort from our entire society" and that "the cornerstone of America's cyberspace security strategy is a public-private partnership."

The Advanced Course in Engineering on Cyber Security (ACE) addressed one component of the National Strategy to Secure Cyberspace by developing the top college students into the next generation of cyber security leaders. Through a public-private partnership among the Air Force Research Laboratory (AFRL), the United States Military Academy (USMA), ITT Corporation and Syracuse University, the ACE followed the proven model of the General Electric Advanced Course in Engineering—formerly known as the Edison course—to transform students into original thinkers, problem solvers and technical leaders.

Far from creating another computer security training program, the pedagogical philosophy underlying the ACE sought to develop leadership skills through problem solving and technical excellence. The following paradigm summarizes best this philosophy: faced with a real-world problem, the graduates of the ACE demonstrated the ability to:

1. formulate a clear problem statement,

2. make reasonable assumptions,

3. apply sound analytical techniques and engineering tools,

4. solve the problem to a certain depth,

5. perform risk analysis on the solution,

6. deliver a solution on time.

This mindset of an engineering leader was best described by Gene Kranz in his book *Failure is not an Option.* As director of mission control at the National Aeronautics and Space Administration (NASA) in the Apollo era, Kranz led his engineers into uncharted territory, the Moon's, and established our unchallenged leadership of space.

Cyberspace in the twenty-first century proves no less challenging than outer space in the twentieth century, and our national security relies on establishing and maintaining unchallenged leadership in cyberspace. The ACE develops cyber security leaders by selecting the top college students in US colleges, providing them with one-on-one mentoring by nationally recognized cyber security leaders from academia, industry and government, and educating them to solve real-world problems in cyber security.

## 3 Methods, Assumptions, and Procedures

The ACE sought to develop the college students into cyber security leaders through a three-pronged approach:

1. developing problem solving skills and on-time performance,

2. communication through sound technical writing and compelling presentations, and

3. mentoring by experienced cyber security professionals.

The rhetorical question on whether leaders are born or developed may be answered by looking at a four-minute miler. While genetics play a pivotal role in breaking the four-minute barrier, it takes years of hard training to prepare for the feat. Similarly, by starting with college students committed to serving this Nation and who have demonstrated leadership qualities, and by equipping them with the tools to solve a series of real-world problems of increasing complexity, we set-up for success in transforming them into the next generation of cyber warriors.

Effective communication is arguably a distinguishing trait of a leader. Therefore, the ACE focused on developing the students into effective communicators by requiring individual weekly written reports, and several structured team presentations. The instructors and the ACE director evaluated student reports and the presentations, and provided detailed feedback and constructive criticism. Appendix A contains the standard grading template, and Appendix B contains a writing guide.

The course met once a week for a full day on Mondays. A typical class started with the timely submission of written reports, security brief by a graduate assistant, and the oral presentation of solutions for the previous week's problem. Students discussed their solutions with the ACE Director and the instructor, before moving on to a new problem. Each week brought a different instructor, who assigned a substantial real-world problem, then lectured for six hours on the background material for that topic.

Finally, students were assigned to work with mentors at local government cyber security laboratories. This mentoring relationship exposed the students to practical challenges of cyber security, and permitted them to establish professional relationships with domain experts.

## 3.1 Curricular Outline and Schedule

The duration of the ACE was ten weeks during the June-August timeframe. Each week focused on one area of cyber security. To make room for important emerging topics (e.g., Cyber Craft), some changes in the content and structure of the curriculum appeared over the course of the project. The 2007 version of the ACE curriculum included the following nine lectures:

1. Cybercraft: agent based networking, trust relations with agents, theory and architecture, command and control of cybercraft.

2. Malicious Code: define the various types and historical examples of malicious code, worm propagation and detection, design and implementation of worms and malicious code propagation.

3. Network Attack: port scanners and packet sniffers, Internet Protocol (IP) spoofing, identifying vulnerabilities, designing and implementing network attacks, red teaming, buffer overflow and malware.

4. Network Defense: host and network firewalls and periphery intrusion detection systems, network monitors and traffic analyzers, network logfiles, patches, TCP(Transmission Control Protocol)-wrappers, encryption stateless and stateful packet-filtering firewalls.

5. Network Forensics: procuring and analyzing digital evidence, preserving the chain of custody of digital evidence, evidence preservation, recovering hidden data on hard drives, classifying file systems, one-way hashes, digital signatures and steganography.

6. Steganography: data hiding in multimedia (images, audio, video), classifying steganography algorithms and tools, steganographic capacity, detection and recovery of hidden data, digital data watermarking, watermark robustness, digital data forensics.

7. Covert Channels: Third Wave society, timing and storage channels, protocol steganography, TCP/IP covert channels and communication, transform and spread spectrum techniques.

8. Access Methods: discrete math and propositional logic, trusted authorities, certificates and credentials, access-control logic, isolation and sharing, request, trust assumptions, jurisdiction and certificates.

9. Wireless: IEEE 802.11[a..z], 802.11 vulnerabilities, wireless attacks and tools, intrusion detection, forensics, wardriving, Bluetooth security, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cracking.

For each topic, the instructor in charge assigned a substantial real-world problem that required 40 to 80 hours of team work to solve. Students worked on teams of three to solve each problem, then wrote and submitted individual reports.

## 3.2 Facilities and Resources

Independence Hall—formerly Air Force barracks—permitted housing the students on Griffiss Park. This convenience provided added flexibility to the course, including in-site classroom and laboratory space, and overall a community environment.

All classes were held in the auditorium of the Griffiss Institute, providing convenient access to AFRL facilities and laboratories.

### 3.3 Faculty and Staff

The faculty for ACE comprised domain-subject experts drawn from government, academia, and industry. Although there were some changes in lecture topics and accompanying faculty members, the faculty remained relatively constant over the course of this project. The following individuals constituted the faculty of the 2007 ACE:

- Maj David Bibighaus – AFRL
- Dr. Kamal T. Jabbour– AFRL
- Maj Paul Williams – Air Force Institute of Technology (AFIT)
- Dr. Gilbert Peterson – AFIT
- Mrs. Sonja Glumich, AFRL
- Dr. Lisa Marvel – Army Research Lab (ARL)
- Chad Heitzenrater – AFRL
- Dr. Steve Chapin – Syracuse University
- Dr. Shiu-Kai Chin – Syracuse University
- Dr. Susan Older – Syracuse University
- LTC Ronald Dodge – USMA
- LT Chad Korosec – United States Naval Reserve (USNR)
- Paul Ratazzi – AFRL
- Col Fred Wiener – United States Air Force (USAF) Ret
- Col Bill Gray – USAF Ret

### 3.4 Reporting

The ACE staff and faculty met each spring to discuss the results of each previous ACE offering and to identify any necessary or desirable changes to the curriculum and program.

The ACE staff then also traveled to various constituents to discuss the results and to recruit for the program. These visits included universities across the United States, where they met with Reserve Officers' Training Corps (ROTC) cadre and cadets. In 2005, the ACE became a sanctioned professional development training (PDT) opportunity for cadets.

## 4 Results and Discussion

Since the inaugural offering of the ACE in summer 2003, the ACE Program has graduated one hundred and fifty five (155) students:

- 119 cadets
- 22 civilians
- 14 National Science Foundation Scholarship for Service recipients.

A paper describing the ACE program's initial (2003) offering [JO04] was presented at the Sixth Workshop on Education for Computer Security (WECS) in 2004. A paper describing the educational objectives and assessment of the access-methods lectures [CO06] was presented at the first Annual Conference on Education in Information Security in 2006.

## 5 Conclusions

Syracuse University completed the requirements for this cooperative agreement, and successfully delivered a turn-key summer Advanced Course in Engineering on Cyber Security at the Rome Research Site. We recruited and selected students, developed the curriculum, hired the faculty, delivered the instruction and evaluated the students. In addition, we placed the students in internship at the lab and affiliated contractors, where they worked on projects related to cyber security challenges of Homeland Security.

## References

[CO06] Shiu-Kai Chin and Susan Older. A rigorous approach to teaching access control. In *Proceedings of the First Annual Conference on Education in Information Security*, Ames, Iowa, 2006. ACM.

[JO04] Kamal Jabbour and Susan Older. The advanced course in engineering on cyber security: A learning community for developing cyber-security leaders. In Cynthia Irvine and Matthew Rose, editors, *Avoiding Fear, Uncertainty and Doubt Through Effective Security Education*, Sixth Workshop on Education for Computer Security (WECS), pages 57–63, Monterey, CA, July 2004. Center for Information Systems Security Studies and Research, Naval Postgraduate School. ISBN 0-9755139-0-7.

## A Standard Grading Template

Appears on next page.

# ADVANCED COURSE IN ENGINEERING
# 2006 Cyber Security BOOT CAMP

## Report Grading Template

Name:

Team:

Lecturer:

Lecture Topic:

Lecture Date:

| | | |
|---|---:|---|
| Cover Page | /10 | |
| Executive Summary | /10 | |
| Problem Statement | /10 | |
| Background | /10 | |
| Assumption | /10 | |
| Tools and Techniques | /10 | |
| Solutions | /20 | |
| Risk Analysis | /10 | |
| References | /10 | |
| **Total** | **/100** | |

ADVANCED COURSE IN ENGINEERING

CYBER SECURITY BOOT CAMP

# ACE Report Writing Guide

by

DR. KAMAL T. JABBOUR, ST

7 June 2004
Revised 29 May 2005
Revised 18 March 2006
Revised 4 June 2007

## 1. Guiding Principles

The ACE writing style seeks to achieve clarity of communication through brevity and simplicity. It promotes short sentences, direct voices and active verbs. It favors past and present tenses over subjunctives. It avoids excessive punctuation, and banishes sentence breaks and sidetracks.

The structure of an ACE report follows the guiding structure of the course. Given a problem, engineers must:

i- formulate a clear problem statement
ii- make reasonable assumptions
iii- apply analytical techniques and computer tools
iv- solve the problem to a certain depth
v- perform risk analysis on the solution, and
vi- deliver the solution on time.

Hence, the ACE report documents the thought process and work effort to solve the problem at hand.

## 2. Report Structure

An ACE report consists of the following parts:

**i-** **Cover Page** – includes the ACE header, an informative title, the name of the author, the name of the team, the names of the members of the team and the date of the report. This writing guide includes a representative cover page.

**ii-** **Executive Summary** – one page long, consists of three paragraphs. The first paragraph states the problem, the second paragraph outlines bounding assumptions, and the third paragraph presents the solution. The executive summary must stand alone as a self-contained document. It may not refer to material in the main body of the report.

**iii-** **Problem Statement –** about one page long, states clearly the problem at hand. It assumes that the reader cannot access the problem statement of the instructor, and presents all the necessary elements of the problem.

**iv-** **Background –** this chapter permits the writer to situate the problem and the solution within the broader field of knowledge. Background information includes reference to prior art and publications, introduces relevant material, and argues the significance of the problem in the broader field of cyber security.

**v-** **Assumptions –** the author states and explains the assumptions that bound the solution space for the problem. The time constraint of the ACE requires a problem solution to a certain depth, and often prevents the engineer from delivering an exhaustive, let alone elegant solution. The assumptions seek to bound the problem statement and the solution space to permit a meaningful solution within the allotted time.

**vi-** **Techniques and Tools –** presents the skill set necessary to solve the problem, includes analytical techniques and computer tools. If the problem requires some skills beyond a high school education, the author lists such skills in this chapter.

**vii-** **Problem Solution** – this chapter contains the meat of the report. It presents the solution to the problem, includes procedures and processes, flow charts and diagrams, results and conclusions.

**viii-** **Risk Assessment** – in this short chapter, the author revisits the assumptions, estimates their possible impact on the solution, and identifies potentially catastrophic oversights.

**ix-** **References** – this final chapter includes a list of three-to-five references, showing the name of the authors, document title, publication, date and place of publication.

## 3. Report Format

### 3.1 Construct hierarchy:

A report consists of named chapters (1, 2, 3). A chapter contains titled sections (2.1, 2.2). A section comprises paragraphs. A paragraph connects sentences. A sentence communicates activity.

Within this iterative hierarchy, each element exhibits the ternary structure of actor, act and action. Thus, a sentence communicates the activity of a subject, a verb and an object. A paragraph connects two-to-three sentences to introduce, explain and clarify a thought. A section comprises three or more paragraphs to summarize its content, elaborate on the details, and conclude the thought.

A chapter starts with an introductory section that reviews the previous paragraph and overviews the current chapter, presents material in the middle sections, and concludes with a section that reviews the chapter and previews the next chapter. Finally, a report starts with a preview chapter (formulate a clear problem statement), presents a solution, and concludes with an assessment.

### 3.2. A matter of style:

For consistency and uniformity, we require all reports to use Times New Roman font size 12. You may use bold font and underscoring to highlight section headings. On the cover page, you may use larger fonts for effect.

Use the dotted decimal numbering system for paragraphs and sections. Do not number the Executive Summary. Assign chapter number 1 to the problem statement.

Write your reports on single sided papers, double-spaced lines and one-inch margins on all four sides of the text. Staple the report on the top left corner, and number the pages on the bottom right corner.

Precede a chapter with two blank lines. Precede a section with one blank line. Do not indent or right-justify your paragraphs.

Number sequentially your references, and surround them with square brackets within your text [1]. Do not use footnotes, they belong to the social sciences.

### 3.3 A matter of substance:

Strive to include a subject, a verb and an object in every sentence. If a sentence contains two verbs, separate its parts with a comma. Limit your use of commas to no more than one comma per sentence.

The devil lies in the punctuation. You must use a period at the end of each sentence. You may use a comma to separate two actions within a sentence, or to separate the first two items in a list of three. Do not use colons, semicolons, exclamation marks or question marks.

Strive to maintain sentence integrity. Avoid parentheses and brackets, and do not split two thoughts with a dash.

Do not use apostrophes.

Avoid using quotation marks. Use your own words to cite a reference.

Do not start a sentence with the words *“and”, “but”* or*” because*”. Do not end a sentence with a preposition, such as *“to”, “of”, “in”, “on”, “into”, “onto”, “under”, “over”, “about’, “for”* or *“from”.*

Avoid statements with sweeping categorical adverbs like *“always”, “never”, “any”, “every”, “all”* and *“none”.* They may undermine the credibility of an entire report if proven wrong.

Use with care quantitative adverbs like *“few”, “some”, “many”* and *“most”.*

Do not sell yourself short. Do not describe your work as “*easy”, “simple”, “straight forward”, “trivial” or “elementary”* (unless your last name is Holmes).

### 3.4 Verb rules:

Use active voice verbs only. Do not use the passive voice. Attribute clearly the responsibility for action and thought.

Use the first person or the third person, and avoid the second person.

Use the present tense or the simple past tense only. Do not use future, present progressive or past progressive tenses.

Do not mix tenses in the same paragraph, let alone in the same sentence. Use the present tense to describe activity, and use the past tense to report data and facts.

Do not use verbs in the *present participle* (verbs that end *“ing”*) since they describe ongoing action.

Avoid adjectives that end with *“ly.”*

Avoid weak verbs "*be", "have", "can" or " do"*. Use verbs that describe state and action.

Do not use "c*ould", "would" or " should."* Use *"must"* or *"shall"* to describe a requirement.

### 3.5 The bottom line:

Use a spell checker and a grammar checker. Seek readability. For example:

The sentence *"Be."* scored 100% on readability and a grade level 0.

The sentence *"Existentialism provided unsatisfactory explanations."* scored 0% on readability and a grade level 12.

## 4. Presentation Format

Use Microsoft PowerPoint to present your work.

Use Arial yellow font size 48 for slide titles, and Arial white font size 32 for the text. Use a navy blue background.

Limit your material to no more than 7 lines per slide.

Aim to balance slide content between concise bullets and runaway sentences.

Avoid tables, equations and quotations. Use charts when appropriate.

## 5. Conclusion

Seek clarity and simplicity in your reports. Aim to communicate substance, not to impress with style. Eliminate spelling, typographical and grammatical errors. A simple report stands a better chance of communicating your message than a sophisticated report without substance.